

(43)Date of publication of application : 28.09.2001

(51)Int.Cl. H04L 9/32  
G06F 15/00  
H04Q 7/38

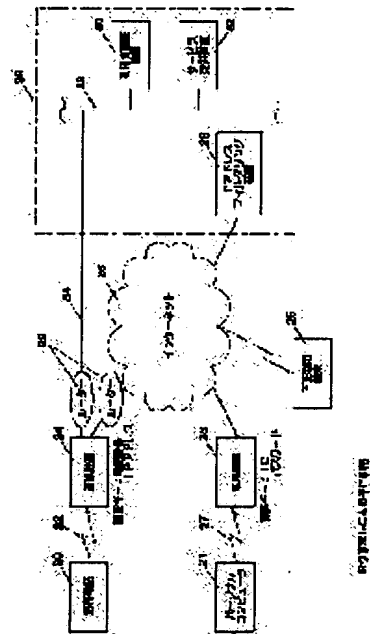
(21)Application number :	2000-075555	(71)Applicant :	KYOCERA COMMUNICATION SYSTEMS CO LTD
(22)Date of filing :	17.03.2000	(72)Inventor :	MIYAHIRO EIICHI OSAKO TETSUO

**(54) USER AUTHENTICATION SYSTEM**

**(57)Abstract:**

**PROBLEM TO BE SOLVED:** To provide a user authentication system that can prevent unauthorized use.

**SOLUTION:** When a mobile phone 20 receives provision of a service of a service provision unit 32, a telephone number and an IP address as an authentication key sent from the mobile phone 20 are transmitted to a user authentication unit 30 via the Internet 26 or a leased line 34. An IP address filtering unit 28 receiving the authentication key via the Internet 26 does not transmit the authentication key to the user authentication unit 30 if the authentication key includes an IP address given by a converter 24. The authentication key sent via the leased line 34, on the other hand, is transmitted to the user authentication unit 30, which authenticates the user. Even when an unauthorized user tries to use the system in a way of a pretended mobile phone user by acquiring the authentication key transmitted through the Internet 26, the IP address filtering unit 28 does not transmit the authentication key to the user authentication unit 30.



## LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision]

of rejection]

[Date of requesting appeal against examiner's  
decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2001-268075 ✓  
(P2001-268075A)

(43) 公開日 平成13年9月28日 (2001.9.28)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テ-7コード (参考)
H 0 4 L 9/32		G 0 6 F 15/00	3 3 0 C 5 B 0 8 5
G 0 6 F 15/00	3 3 0	H 0 4 L 9/00	6 7 3 B 5 J 1 0 4
H 0 4 Q 7/38		H 0 4 B 7/26	1 0 9 R 5 K 0 6 7

審査請求 未請求 請求項の数 8 O L (全 12 頁)

(21) 出願番号 特願2000-75555(P2000-75555)

(22) 出願日 平成12年3月17日 (2000.3.17)

(71) 出願人 596100812  
京セラコミュニケーションシステム株式  
社  
京都市山科区東野北井ノ上町5番地の22  
(72) 発明者 宮廣 栄一  
京都府京都市山科区東野北井ノ上町5番地  
の22 京セラコミュニケーションシステム  
株式会社内  
(74) 代理人 100092956  
弁理士 古谷 栄男 (外2名)

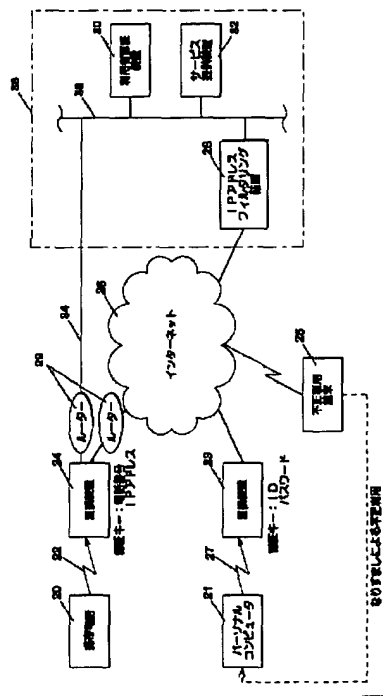
最終頁に続く

(54) 【発明の名称】 利用者認証システム

(57) 【要約】

【課題】 不正利用を防止することのできる利用者認証システムを提供する。

【解決手段】 携帯電話20によって、サービス提供装置32のサービスの提供を受ける場合、携帯電話20から送信された認証キーとしての電話番号とIPアドレスは、インターネット26または専用線34を介して利用者認証装置30に向けて送信される。インターネット26経由で認証キーを受信するIPアドレスフィルタリング装置28は、その認証キーが変換装置24で付与されたIPアドレスを含んでいれば、その認証キーを利用者認証装置30に送信しない。一方、専用線34経由で送信された認証キーは送信されて利用者認証が行われる。インターネット26上を流れるその認証キーを取得することにより携帯電話へのなりすまし不正利用をしても、IPアドレスフィルタリング装置28はその認証キーを利用者認証装置30に送信しない。



## 【特許請求の範囲】

## 【請求項 1】端末装置、

端末装置に対して専用線を介して接続された識別情報付加装置、  
識別情報付加装置に対して通信路を介して接続された識別情報選択送信装置、  
識別情報付加装置に対して専用線を介して接続されるとともに識別情報選択送信装置に対しても専用線を介して接続された利用者認証装置、  
を備えた利用者認証システムであって、  
端末装置は、  
識別情報付加装置に対して利用者情報を送信する利用者情報送信手段を備え、  
識別情報付加装置は、  
端末装置から送信された利用者情報に対して識別情報を付加する識別情報付加手段と、  
識別情報付加手段によって得られた利用者識別情報を通信路を介して識別情報選択送信装置に向けて送信する通信路経由利用者識別情報送信手段と、  
前記利用者識別情報を専用線を介して利用者認証装置に対して送信する専用線経由利用者識別情報送信手段とを備え、  
識別情報選択送信装置は、  
識別情報付加装置が付加する識別情報を含んだ利用者識別情報は利用者認証装置に送信しないが前記識別情報以外の識別情報を含んだ利用者識別情報は利用者認証装置に送信する利用者識別情報選択送信手段を備え、  
利用者認証装置は、  
識別情報付加装置または識別情報選択送信装置から専用線を介して送信される利用者識別情報を受けて利用者認証を行う利用者認証手段、  
を備えたことを特徴とする利用者認証システム。

【請求項 2】請求項 1 の識別情報付加装置において、さらに、  
利用者識別情報を通信路を介して識別情報選択送信装置に向けて送信するかまたは専用線を介して利用者認証装置に対して送信するかのいずれかを選択する送信経由選択手段、  
を備えたことを特徴とするもの。

【請求項 3】識別情報付加装置に対して通信路を介して接続されるとともに、利用者認証装置に対して専用線を介して接続された識別情報選択送信装置において、  
識別情報付加装置が付加する識別情報を含んだ利用者識別情報は利用者認証装置に送信しないが前記識別情報以外の識別情報を含んだ利用者識別情報は利用者認証装置に送信する利用者識別情報選択送信手段、  
を備えたことを特徴とする識別情報選択送信装置。

【請求項 4】請求項 1～3 のいずれかの識別情報選択送信装置において、さらに、  
識別情報付加装置が付加する識別情報を記憶した記憶

部、  
を備えており、  
識別情報選択送信手段は、前記記憶部を参照することによって、利用者認証装置に送信する利用者識別情報と送信しない利用者識別情報とを選択することを特徴とするもの。

【請求項 5】請求項 4 の利用者認証システムにおいて、  
識別情報付加装置が付加する識別情報が更新された場合には、

10 識別情報付加装置は、さらに、  
更新された識別情報を専用線を介して識別情報選択送信装置に対して送信する更新識別情報送信手段を備え、  
識別情報選択送信装置は、さらに、  
前記記憶部の更新を前記送信された更新識別情報に基づいて行う選択送信識別情報更新手段、  
を備えたことを特徴とする利用者認証システム。

【請求項 6】請求項 1～5 のいずれかの利用者認証システムにおいて、  
識別情報選択送信装置と利用者認証装置が一体の装置として構成されていることを特徴とする利用者認証システム。

【請求項 7】請求項 1～6 において、  
識別情報は、IP アドレスであることを特徴とするもの。

【請求項 8】端末装置の利用者を、端末装置に接続された利用者認証装置によって認証する利用者認証方法であって、  
端末装置が利用者認証を受ける際には、  
端末装置からの利用者情報に識別情報を付加して、通信路または専用線経由により利用者認証装置に向けて送  
30 り、  
通信路経由により送られた前記識別情報を有する利用者情報は利用者認証装置に送られず、専用線経由により送られた利用者情報は利用者認証装置に送られ、  
利用者認証装置は、専用線経由により送られた前記利用者情報に基づいて利用者認証を行う利用者認証方法。

## 【発明の詳細な説明】

## 【0001】

【発明の技術分野】この発明はインターネットなどのネットワークを用いてサービスを提供するサービスシステムにおける利用者認証に関するものであり、特に、不正利用防止に関する。

## 【0002】

【従来の技術】図 1 に、インターネットを利用した従来の利用者認証システムを示す。利用者端末 2 は、インターネット利用可能な携帯電話やパーソナルコンピュータ等である。利用者端末 2 は、電話網 14 を介して変換装置 4 に接続されており、変換装置 4 は、インターネット 6 に接続されている。そして、インターネット 6 には、利用者認証装置 8 とサービス提供装置 10 がそれぞれ接続されており、利用者認証装置 8 とサービス提供装

置 10 は LAN 16 で接続されている。

【0003】利用者端末 2 がサービス提供装置 10 のサービスを利用するにあたっては、その前提として利用者認証を行う必要がある。このため、利用者端末 2 は、まず、利用者端末 2 を特定するための識別子を変換装置 4 に送信する。それを受けた変換装置 4 は、ネットワーク上で利用者端末を一意に特定するために、利用者端末 2 に対する IP アドレスの配布と、送信された識別子に IP アドレスを付与したものである認証キーを、電話網からインターネットへのプロトコル変換を行う。そして、変換装置 4 は、認証キーをインターネット 6 を介して利用者認証装置 8 に送信する。その認証キーを受けた利用者認証装置 8 は、利用者認証を行い、認証が終了した後はサービス提供装置 10 が利用者端末 2 に対してサービスの提供を行う。すなわち、利用者認証装置 8 は、利用者端末 2 から送られてくる認証キーが真正なものでなければ利用者の認証を拒否し、真正のものであればサービス利用を許可する。

【0004】ここで、利用者端末としては、インターネット利用可能な携帯電話やパーソナルコンピューター等の仕様が異なる様々なものが存在する。したがって、そのような種々の利用者端末から同じ情報にアクセスする場合を考慮した結果として、利用者認証装置はインターネット経由ですべてのアクセスを取り扱うのが好ましいと考えられる。

【0005】一方、利用者端末がパーソナルコンピューターの場合は、認証キーとしてパスワードや ID が用いられるのが一般的であるが、インターネット利用可能な携帯電話の場合は利用者の操作簡便化のため電話番号により一意に特定される加入者 ID が用いられることがある。

【0006】

【発明が解決しようとする課題】しかしながら、従来の利用者認証システムには次のような問題があった。

【0007】パーソナルコンピューターが認証キーとして送信するパスワードや ID と比較すると、インターネット利用可能な携帯電話が認証キーとして送信する電話番号により一意に特定される加入者 ID は、偽造が比較的に容易な変数としてインターネット上を流れるため、悪意の利用者が、正規の携帯電話の利用者になりすまして不正利用を行う懸念が生じる。

【0008】すなわち、図 1 のインターネット 6 を流れている加入者 ID を不正利用端末 12（不正プログラムを備えたパーソナルコンピューター等）により取得した悪意の利用者が、その不正利用端末 12 を操作して正規の携帯電話の利用者になりすまして利用者認証装置 8 にアクセスしてサービスの提供を受けた場合には正規の利用者が不測の損害を被るおそれがある。特にそのサービスが有料である場合には、不正利用をされた利用者が、サービスの提供を受けていないにもかかわらず料金を負担

しなければならないという事態が懸念されるという問題がある。

【0009】なお、このような問題は、インターネット利用可能な携帯電話と違って、パーソナルコンピューター等は、不正利用者がそのパーソナルコンピューターのプログラムの変更を行うことができる可能性がある、ということ为背景としているものである。

【0010】このような状況は、インターネット利用可能な携帯電話の利用者にとっては不安要因となるものであり、また、今後増加すると予想される、携帯電話によってインターネットを利用したサービスの提供を受けるというシステムの発達を阻害する要因として懸念される。

【0011】この発明は、上記のような問題に鑑みて、不正利用を防止することのできる利用者認証システムを提供することを目的とする。

【0012】

【課題を解決するための手段および発明の効果】（1）この発明の利用者認証システムは、端末装置、端末装置に対して専用線を介して接続された識別情報付加装置、識別情報付加装置に対して通信路を介して接続された識別情報選択送信装置、識別情報付加装置に対して専用線を介して接続されるとともに識別情報選択送信装置に対しても専用線を介して接続された利用者認証装置、を備えた利用者認証システムであって、端末装置は、識別情報付加装置に対して利用者情報を送信する利用者情報送信手段を備え、識別情報付加装置は、端末装置から送信された利用者情報に対して識別情報を付加する識別情報付加手段と、識別情報付加手段によって得られた利用者識別情報を通信路を介して識別情報選択送信装置に向けて送信する通信路経由利用者識別情報送信手段と、前記利用者識別情報を専用線を介して利用者認証装置に対しても送信する専用線経由利用者識別情報送信手段とを備え、識別情報選択送信装置は、識別情報付加装置が付加する識別情報を含んだ利用者識別情報は利用者認証装置に送信しないが前記識別情報以外の識別情報を含んだ利用者識別情報は利用者認証装置に送信する利用者識別情報選択送信手段を備え、利用者認証装置は、識別情報付加装置または識別情報選択送信装置から専用線を介して送信される利用者識別情報を受けて利用者認証を行う利用者認証手段、を備えたことを特徴としている。

【0013】これにより、通信路を流れている利用者識別情報を不正に取得した悪意の利用者が、正規の端末装置の利用者になりすまして利用者認証を受けることを試みた場合でも、利用者認証はされないことになる。

【0014】なぜならば、悪意の利用者が送信する利用者識別情報は、本発明における識別情報付加装置とは別の経由で通信路に送信されることになるのであるから、専用線経由による送信はされない。さらに、その不正に取得した利用者識別情報に含まれる識別情報は、本発明

における識別情報付加装置が付加する識別情報と同一のものであるから、識別情報選択送信装置はその利用者識別情報を利用者認証装置に送信しないからである。

【0015】そして、一方の専用線を流れている利用者識別情報は第三者に取得されることがなく、安全に利用者認証装置に送信される。したがって、なりすましによる不正利用を防止することができる。

【0016】また、通信路と専用線から同じ情報が利用者認証装置に送信されることがないので、利用者識別情報の衝突等といったシステム上の不都合は生じない。

【0017】さらに、利用者識別情報が偽造容易なものであっても不正利用を防止することができるので、利用者識別情報は簡易なものでよい一方で、端末装置の利用者の操作簡便化が図られるとともに、信頼性の高いシステムが構築できる。

【0018】また、従来の利用者認証システムに、専用線と識別情報選択送信装置を設けるだけでよいのであるから、構成がシンプルであり低コストで不正利用の防止をすることができる。

【0019】(2) この発明の識別情報付加装置は、さらに、利用者識別情報を通信路を介して識別情報選択送信装置に向けて送信するかまたは専用線を介して利用者認証装置に対して送信するかのいずれかを選択する送信経路選択手段、を備えたことを特徴としている。

【0020】これにより、専用線を介して利用者識別情報を利用者認証装置に送信する場合には、利用者識別情報の安全性がより確実に確保される。すなわち、利用者識別情報が通信路上を流れた場合には、第三者が不正にその情報を取得する可能性があるが、専用線のみが経路として選択される場合にはそのような危険性はない。

【0021】(3) この発明の利用者認証システムの識別情報選択送信装置は、識別情報付加装置が付加する識別情報を記憶した記憶部、を備えており、識別情報選択送信手段は、前記記憶部を参照することによって、利用者認証装置に送信する利用者識別情報と送信しない利用者識別情報とを選択することを特徴としている。

【0022】したがって、様々な仕様の利用者端末が新たに加わったり、使用されなくなった場合に、識別情報選択送信装置が利用者認証装置に送信しない利用者識別情報の設定や更新を行う際には、記憶部における識別情報の記憶内容の設定や更新のみで対応できる。

【0023】(4) この発明の利用者認証システムは、識別情報付加装置が付加する識別情報が更新された場合には、識別情報付加装置は、さらに、更新された識別情報を専用線を介して識別情報選択送信装置に対して送信する更新識別情報送信手段を備え、識別情報選択送信装置は、さらに、前記記憶部の更新を前記送信された更新識別情報に基づいて行う選択送信識別情報更新手段、を備えたことを特徴としている。

【0024】したがって、識別情報選択送信装置が利用

者認証装置に送信しない利用者識別情報を、新たに設定する場合だけでなく、端末装置の仕様が異なる様々なものが新たに加わったり減ったりした場合においても、その記憶部の記憶内容の更新を簡易かつ迅速に行うことができる。

【0025】また、更新された利用者識別情報は専用線のみを介して識別情報選択送信装置に送信されるから情報の安全性が確保される。すなわち、更新された識別情報が通信路上を流れた場合には、それを取得した第三者がその更新情報に変更を加えたり等することにより本システムが正常に機能しないようにされるおそれがあるが、本発明によればそのような危険性はない。

【0026】(5) この発明の利用者認証システムにおける識別情報は、IPアドレスであることを特徴としている。

【0027】ここで、IPアドレスは、識別情報付加装置が利用者情報に付加するものであり、コンピュータが管理・理解しやすい数字等によって表されるものであるから、識別情報選択送信装置に記憶させる内容の規格が統一化され、識別情報のデータ更新が容易であるとともに記憶容量を少なくすることができ、識別情報選択送信手段の処理を迅速化することができる。

【0028】(6) 用語の定義

この発明において、「端末装置」とは、サービスの提供を受ける側の装置であって、インターネット等のネットワークに接続可能な装置をいう。実施形態では、図2の携帯電話20とパーソナルコンピュータ21の利用者端末がこれに該当する。

【0029】「通信路」とは、無線、有線を問わず、2以上の装置との通信を行うためのものをいい、インターネットのように開放されたものだけでなく、LANのように閉じられたものも含む概念である。実施形態では、図2のインターネット26がこれに該当する。

【0030】「専用線」とは、無線、有線を問わず、2以上の装置との通信を行うためのものをいうが、閉じられた回線のみに限定されインターネットのように開放されたものは含まない概念であり、情報通信を行う2点間が閉じられた回線における電話網、LAN等をいう。実施形態では、図2の電話網22、27、専用線34、LAN36がこれに該当する。

【0031】「利用者情報」とは、端末装置の利用者を特定するために端末装置から送信される識別子であり、電話番号やID、パスワード、デジタル証明書等をいう。実施形態では、図6のステップS1の電話番号がこれに該当する。

【0032】「識別情報」とは、端末装置から送信される電話番号等の識別子に対して付加される情報であり、ネットワーク上で利用者端末を一意に特定するためのアドレスをいう。実施形態では、図6のステップS3のIPアドレスがこれに該当する。

【0033】「識別情報付加装置」とは、実施形態においては図2の変換装置23および24が該当する。

【0034】「利用者識別情報」とは、端末装置の利用者を特定するために端末装置から送信される識別子に対して、ネットワーク上で利用者端末を一意に特定するためのアドレスが付与された情報をいう。実施形態では、図6のステップS5の認証キーがこれに該当する。

【0035】「識別情報選択送信装置」とは、実施形態においては図2のIPアドレスフィルタリング装置28が該当する。

【0036】「送信経路選択手段」とは、実施形態においては図2のルーター29が該当する。

【0037】「識別情報付加装置が付加する識別情報を記憶した記憶部」とは、実施形態においては図7のIPアドレスフィルタリングテーブルが該当する。

【0038】

【発明の実施の形態】(1) 利用者認証システムの実施形態の構成

本発明に係る利用者認証システムの実施形態を図面に基づいて説明する。図2に、この発明の一実施形態による利用者認証システムの構成を示す。携帯電話20とパーソナルコンピュータ21は、利用者端末である。携帯電話20は、電話網22を介して変換装置24に接続されており、パーソナルコンピュータ21は、電話網27を介して変換装置23に接続されている。携帯電話20は、インターネット利用可能であり、パーソナルコンピュータ21は、通常の電話によるダイヤルアップ接続または常時接続によってインターネット利用可能である。つまり、携帯電話20は変換装置24を介して、パーソナルコンピュータ21は変換装置23を介して、それぞれがインターネット26に接続可能となっている。なお、変換装置24には、専用線34またはインターネット26のいずれかの経路を選択するためのルーター29が設けられている一方、利用者認証等を行う、IPアドレスフィルタリング装置28と、利用者認証装置30、サービス提供装置32とは、管理センター38内に設置されており、それぞれの装置は、管理センター38内のLAN36によってお互いに接続されている。また、IPアドレスフィルタリング装置28は、インターネット26とも接続されており、LAN36は、専用線34に接続されている。

【0039】変換装置23、24は、一般的には電話通信事業者によって運営されている。また、管理センター38は、電話通信事業者などの公共性の高い組織やその認定業者などが運営することが好ましい。

【0040】(2) パーソナルコンピュータ21等のハードウェア構成

図3に、パーソナルコンピュータ21のハードウェア構成を示す。パーソナルコンピュータ21は、メモリ40、ディスプレイ42、通信回路44、キーボード／

マウス46、CPU48、ハードディスク(記録装置)50、CD-ROMドライブ52を備えている。また、ハードディスク50には、オペレーティングシステム(マイクロソフト社のWindows98など)、ウェブを閲覧するためのブラウザプログラムが格納されている。このブラウザプログラムは、CD-ROMドライブ52を介して、CD-ROM54からインストールされたものである。通信回路44は、インターネット26に接続するための回路である。

【0041】変換装置23および24、利用者認証装置30、サービス提供装置32も、それぞれ、図3に示すハードウェア構成と同様である。ただし、変換装置23および24においては、ハードディスクにIPアドレスとプロトコル変換プログラムが記録されており、利用者認証装置30においては、ハードディスクに利用者認証プログラムが記録されており、サービス提供装置32においては、ハードディスクにサービス提供のためのサービス提供ウェブサーバープログラムが記録されている。

【0042】(3) IPアドレスフィルタリング装置28のハードウェア構成

図4に、IPアドレスフィルタリング装置28のハードウェア構成を示す。IPアドレスフィルタリング装置28は、表示パネル90、メモリ92、通信回路94、スイッチ96、CPU98を備えている。通信回路94は、インターネット26に接続するための回路である。

【0043】(4) 携帯電話20の構成  
図5に、携帯電話20のブロック図を示す。入出力デバイスとして、液晶ディスプレイ62、テンキー／スイッチ64、マイク66、スピーカ(通話用)68、スピーカ(着信音用)70が設けられている。音声符号化回路74は、マイク66からの音声を送信のために符号化し、受信した音声信号を復号化してスピーカ68から出力するための回路である。マイクロブラウザ72は、記録装置に記録されたプログラムであって、サービス提供ウェブからのデータを閲覧するためのものである。無線通信回路76は、音声やデータを無線通信によって送信または受信するための回路である。シリアルデータ通信回路78は、外部のパーソナルコンピュータ84との通信を行うための回路である。メモリ80には、利用者自身の電話番号、電話帳などが記録されている。制御回路86は、これらの回路を制御する。また、バッテリー82は、各部に電源を供給する。

【0044】(5) 携帯電話20から利用者認証を受ける場合の処理

図6に、利用者端末としての携帯電話20から利用者認証を受ける場合の処理を示す。この処理は利用者端末がサービス提供装置32からサービスの提供を受ける際の前提となるものである。

【0045】まず、利用者は、携帯電話20を操作して変換装置24に接続し、利用者認証装置30への接続要求と利用者認証のための識別子である電話番号を送信す

る(ステップS1)。変換装置24は、これを受けて接続許可(ステップS2)と、電話番号に対するIPアドレスの付与(ステップS3)と携帯電話20に対するIPアドレスの配布(ステップS4)を行う。ここで、変換装置24は、携帯電話20に対して配布するIPアドレスをあらかじめハードディスクにプールしており、携帯電話20からの接続要求がある度毎にそのプールしているIPアドレスから空いているものを選択して配布している。

【0046】そして、識別子である電話番号は、加入者IDに変換されるとともに(ステップS5)、電話網からインターネットプロトコルへプロトコル変換される(ステップS6)。ここで、加入者IDは、通信事業者が、利用者の電話番号と一意に対応づけて付与している識別子である。そして、認証キーとしての、加入者IDとIPアドレスは、専用線34とLAN36を介して利用者認証装置30に送信される(ステップS7)。

【0047】このとき、変換装置24は、前記認証キーをインターネット26には送信しない。これは、変換装置24に設けられたルーター29によるものである。すなわち、前記ステップS1の接続要求に含まれるあて先のIPアドレスが、利用者認証装置30やサービス提供装置32のアドレスであれば、認証キーの送信経路として専用線34のみを選択するようにルーター29が設定されていることによる。

【0048】したがって、携帯電話20から送信された認証キーは、専用線34経由(ステップS7)のみで利用者認証装置30に送信されて利用者認証が行われる(ステップS11)。

【0049】(6)なりすましによる不正利用の防止について

次に、本実施形態の構成により、携帯電話の利用者へのなりすましによる不正利用を防止できることを説明する。

【0050】ここで、携帯電話の利用者へのなりすましによる不正利用は、正規に利用者認証されるべき携帯電話20の利用者が本システム以外の他のインターネットサービス等を利用するときに、インターネット26上に送信されることになる認証キーを、パーソナルコンピュータ等の不正利用端末25を操作する悪意の利用者が取得することによって行われる。つまり、不正利用端末25を操作する悪意の利用者は、インターネット26上を流れる認証キーとしての加入者IDとIPアドレスを、不正利用端末25内の不正プログラムによって取得・解読する。そして、パーソナルコンピュータ等の不正プログラムにより、あたかもその取得した加入者IDとIPアドレスが発信元であるかのようになりすまして変換装置23にアクセスをし、変換装置23から本来割り当てられるIPアドレスとは異なるIPアドレスとして、不正にインターネットに侵入すること等によって行われる。

【0051】しかし、そのようななりすましの不正利用

によるサービスの提供を受けることを試みた場合でも、その認証キーは利用者認証装置30には送信されない。

【0052】これは、以下に説明するIPアドレスフィルタリング装置28の構成によるものである。

【0053】IPアドレスフィルタリング装置28は、送信された認証キーを受けてフィルタリングを行う。これは、IPアドレスフィルタリング装置28のメモリ92に記憶されている、図7に例示するようなIPアドレスフィルタリングテーブルを参照して行うものである。

【0054】図7のIPアドレスフィルタリングテーブルには、Reject(禁止)のActionをする場合の、発信元のIPアドレスのカラムが記録されており、このIPアドレスは変換装置24がプールしているIPアドレスと同一である。このReject(禁止)のActionは、認証キーがインターネット26から送信された場合、その認証キーがカラムに記録されたものと同一のIPアドレスを含んでいれば、その認証キーを利用者認証装置30に送信しないという動作を行わせるものである。例えば、図7のIPアドレスフィルタリングテーブルにおいては、認証キー中の発信元のIPアドレスが、192.168.1.5であればその認証キーは利用者認証装置30には送信されない。一方、認証キー中の発信元のIPアドレスが、193.100.1.1であればその認証キーは利用者認証装置30に送信されることになる。

【0055】これにより、パーソナルコンピュータ等による携帯電話の利用者へのなりすましの不正利用で認証キーを送信しても、それを受ける変換装置23はその認証キーをインターネット26のみを経由して利用者認証装置30に向けて送信する一方で、その認証キーは、IPアドレスフィルタリングテーブル中に記録されている、本来携帯電話20に割り当てられるIPアドレスを含んでいるため、それを受信したIPアドレスフィルタリング装置28はその認証キーを利用者認証装置に送信しない(ステップS9)。すなわち、利用者認証はされないことになる。

【0056】(7)本実施形態による効果について  
以上のように、本実施形態によれば、パーソナルコンピュータ等による携帯電話の利用者へのなりすましの不正利用を防止することができる。

【0057】また、インターネット26と専用線34から同じ情報が利用者認証装置30に送信されることがないので、IPパケットの衝突等といったシステム上の不都合は生じない。

【0058】さらに、利用者認証のために送信する情報が加入者IDやIPアドレスである場合のように比較的偽造容易なものであっても不正利用がされないので、特別に携帯電話を操作してパスワードを送信する等の手間の必要がなく利用者の操作簡便化が図られるとともに、信頼性の高いシステムが構築できる。

【0059】そして、従来の利用者認証システムに専用



線とIPアドレスフィルタリング装置を設けるだけでよいのであるから、構成がシンプルであり低コストで不正利用の防止ができる。

【0060】さらに、変換装置24に設けられたルーター29により、専用線34が経由として選択された場合には認証キーの安全性がより確実に確保される。すなわち、認証キーがインターネット26上を流れた場合には、第三者が不正にその認証キーを取得する可能性があるが、専用線34のみが経由として選択される場合にはそのような危険性はない。

【0061】なお、専用線34が経由として選択されて利用者認証がされた場合に、利用者認証終了後の携帯電話20に対する情報の送信を行う経路としては管理センター38内の専用線34を使用するのが通常である。かかる場合に、専用線34の通信トラフィックに負荷がかかる可能性があるが、その負荷を分散するために以下のような構成を採用することもできる。

【0062】例えば、利用者認証装置30やサービス提供装置32のCPU等の制御により、それらが送信する情報送信量等に一定の制限値を設けておき、情報送信量等がその制限値を越える場合には情報送信経路としてインターネット26を選択させることによって専用線34の通信トラフィックの負荷を分散させることができる。また、本実施形態においては示していないが、管理センター38内のLAN36と、専用線34およびインターネット26とを中継する複数のルーターを備えることによって、ルーター間で互いに遅延時間等をやり取りさせ、携帯電話20に対する情報の送信を行う経路として、専用線34またはインターネット26のいずれが最適かを選択させることによって専用線34の通信トラフィックの負荷を分散させることができる。これにより、携帯電話20の利用者数が増加した場合にも、迅速かつ安定したシステムの運営が可能である。

【0063】また、IPアドレスフィルタリング装置28は、IPアドレスフィルタリングテーブルを備えているから、様々な仕様の携帯電話が新たに加わったり使用されなくなった場合に、IPアドレスフィルタリング装置28が利用者認証装置30に送信しない認証キーの設定や更新を行う際には、IPアドレスフィルタリングテーブルの記憶内容の更新のみで対応できる。

【0064】ここで、IPアドレスは、変換装置24にあらかじめプールされたものであり、コンピューターが管理・理解しやすい数字等によって表されるものであるから、IPアドレスフィルタリング装置28に記憶させる内容の規格が統一化され、IPアドレスフィルタリングテーブルの記憶内容の更新が容易であるとともに、記憶容量を少なくすることができ、IPアドレスフィルタリング装置のフィルタリング処理を迅速化することができる。

【0065】なお、本実施形態におけるIPアドレスフィルタリングテーブルには、Reject（禁止）するものの発

信元のIPアドレスのカラムを記録しているが、これに限定されるものではない。例えば、Accept（送信する）のActionを指令するカラムや、あて先のIPアドレスのカラム、対象サービス（TCPポート番号）のカラムをこのテーブルに併せて記録してもよい。このようにした場合には、あて先のIPアドレスのカラムには、利用者認証装置30やサービス提供装置32内のサービス提供ウェブに割り当てられているIPアドレス等を、対象サービスのカラムには、httpやmail等のサービスの種類を記録することができる。

【0066】なお、本実施形態においては、変換装置24にルーター29が設けられている場合を説明したが、ルーターを設けていない場合であっても本システムは実施可能である。なぜならば、この場合変換装置24は、認証キーを専用線34経由だけでなくインターネット26経由にも送信することになるが、インターネット26経由で認証キーを受けるIPアドレスフィルタリング装置28は、上述したように、変換装置24が付与するIPアドレスを含んだその認証キーを利用者認証装置30に送信しないのであるから、結果として上記実施形態と同様の効果を奏することになるからである。

【0067】（8）パーソナルコンピューター21から利用者認証を受ける場合の処理

パーソナルコンピューター21が利用者認証を受ける場合の構成では、図2に示すように、パーソナルコンピューター21に接続された変換装置23はインターネット26のみに接続され、携帯電話20の場合と違って専用線34の経由による認証キーの送信はない。

【0068】また、利用者認証のための識別子としては、IDとパスワードが要求されることが多い。これは、パーソナルコンピューターにはキーボードが通常備えられているから、利用者がIDやパスワードの入力を容易に行うことができる一方で、利用者認証をより確実に行うためである。

【0069】パーソナルコンピューター21から利用者認証を受ける場合の処理では、変換装置23は、利用端末が携帯電話である場合と同様に、認証キーを受けて、接続許可と認証キーに対するIPアドレスの付与、パーソナルコンピューター21に対するIPアドレスの配布とを行う。そして、認証キーはプロトコル変換され、インターネット26を介してIPアドレスフィルタリング装置28に送信される。このとき、そのIPアドレスはIPアドレスフィルタリングテーブルに含まれているものとは同一ではないから、LAN36を介して利用者認証装置30に送信されることになる。これは、すなわち、IPアドレスフィルタリング装置内のIPアドレスフィルタリングテーブルには、変換装置24にプールされているIPアドレスが記録されており、一方の変換装置23にプールされているIPアドレスが記録されていないのであるから、パーソナルコンピューターを発信元とする認証キーは、IP

アドレスフィルタリング装置 28 による、送信しない（禁止）という動作の対象にならないことによるものである。

【0070】このように、本実施形態においては、携帯電話 20 が利用者端末の場合には専用線 34 を経由して認証キーを送信等することによってなりすましによる不正利用を防止している一方で、パーソナルコンピュータ 21 が利用者端末の場合には専用線 34 経由による認証キーの送信をしていない。これは、上記のように、携帯電話の場合は、利用者認証のために送信する認証キーが加入者 ID や IP アドレスのように比較的偽造容易なものだからである。したがって、実施形態としてはこれに限られるものではない。例えば、使用される認証キーが偽造容易である等の事情により、なりすましによる不正利用がなされる懸念のあるその他の端末装置であっても、本実施形態における、携帯電話 20 から利用者認証を受ける場合の構成と同様の構成を採用することにより不正利用を防止することができる。

【0071】(9) IP アドレスフィルタリング装置 28 の IP アドレスフィルタリングテーブルの記録内容を更新する場合の処理

図 8 に、IP アドレスフィルタリング装置 28 の IP アドレスフィルタリングテーブルの記録内容を更新する場合の処理を示す。携帯電話 20 から送信される電話番号に対して、変換装置 24 が付与する IP アドレスが増えたり減ったりした等の更新があった場合には、変換装置 24 のプールする IP アドレスが更新される（ステップ S 50）。そして、変換装置 24 のハードディスクのプログラムによって、更新された IP アドレスのデータが専用線 34 と LAN 36 を介して IP アドレスフィルタリング装置 28 に送信され（ステップ S 51）、更新された IP アドレスのデータを受信した IP アドレスフィルタリング装置 28 は、IP アドレスフィルタリングテーブルの内容の更新を行う（ステップ S 52）。

【0072】したがって、IP アドレスフィルタリング装置 28 が利用者認証装置 30 に送信しない認証キーを、新たに設定する場合だけでなく、携帯電話の仕様が異なる様々なものが新たに加わったり減ったりした場合においても、IP アドレスフィルタリングテーブルの記憶内容の更新を簡易かつ迅速に行うことができる。

【0073】また、更新された IP アドレスのデータは、専用線 34 と LAN 36 のみを介して IP アドレスフィルタリング装置 28 に送信されるから、データの安全性が確保される。すなわち、更新された IP アドレスがインターネット 26 上を流れた場合には、それを取得した第三者が不正利用端末 25 を操作してそのデータに変更を加えたりする等することにより本システムが正常に機能しなくなるようにされるおそれがあるが、本実施形態によればそのような危険性はない。

#### 10 【図面の簡単な説明】

【図 1】従来の利用者認証システムを示す図である。

【図 2】本発明の一実施形態による利用者認証システムを示す図である。

【図 3】利用者端末としてのパーソナルコンピュータのハードウェア構成を示す図である。

【図 4】IP アドレスフィルタリング装置のハードウェア構成を示す図である。

【図 5】利用者端末としての携帯電話のブロック図を示す図である。

20 【図 6】利用者認証を受ける場合の処理を示す図である。

【図 7】IP アドレスのフィルタリングテーブルの内容を示す図である。

【図 8】IP アドレスフィルタリング装置の IP アドレスフィルタリングテーブルの記録内容を更新する場合の処理を示す図である。

#### 【符号の説明】

20・・・携帯電話

21・・・パーソナルコンピュータ

30 23、24・・・変換装置

28・・・IP アドレスフィルタリング装置

30・・・利用者認証装置

32・・・サービス提供装置

38・・・管理センター

29・・・ルーター

22・・・電話網

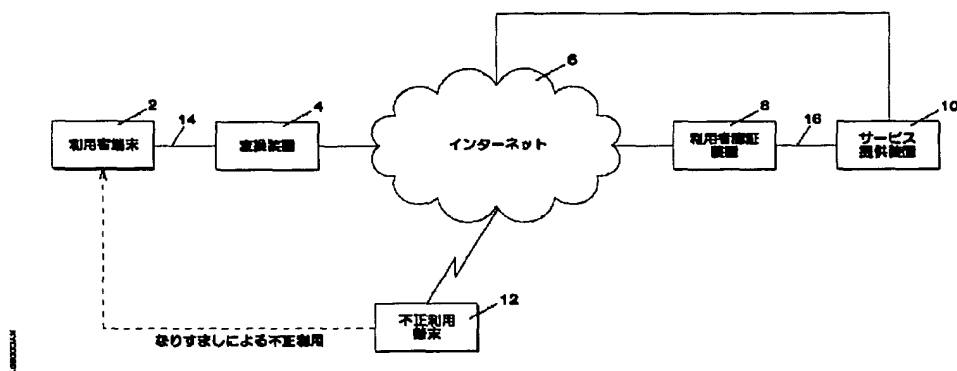
26・・・インターネット

34・・・専用線

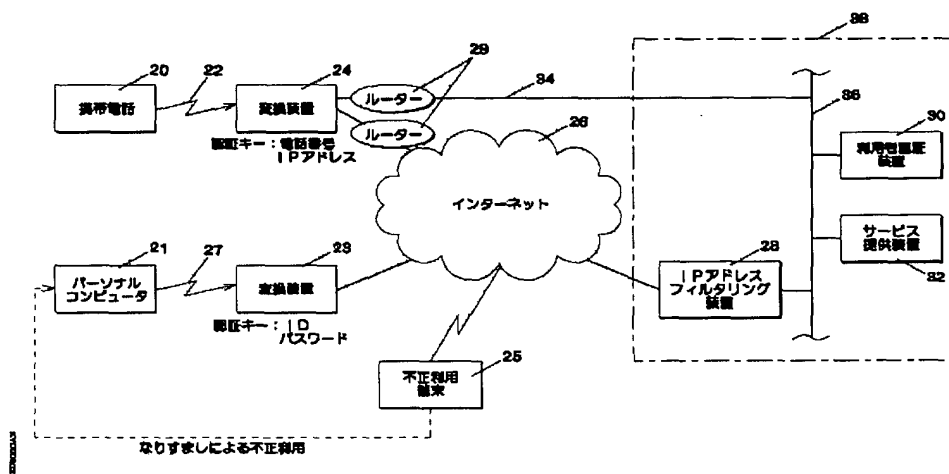
36・・・LAN

40 25・・・不正利用端末

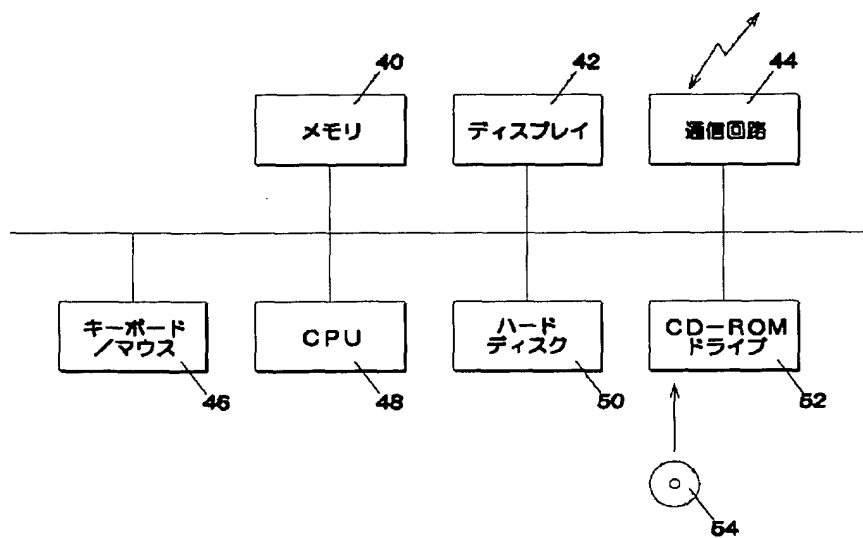
**MYCOTOXINS**



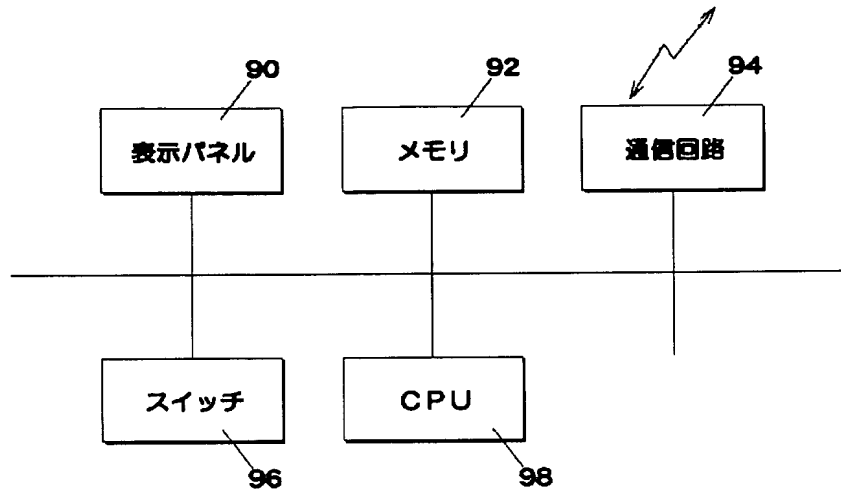
**SYNOPSIS**



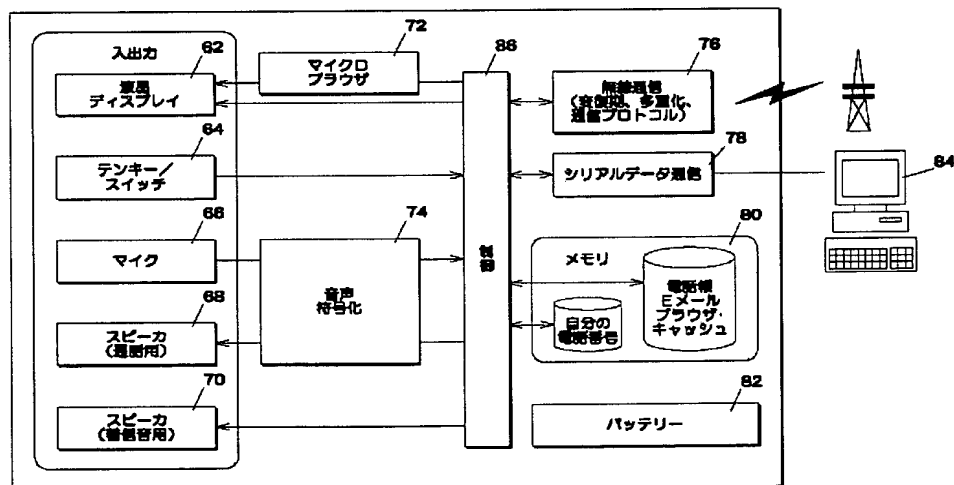
**Keywords:**



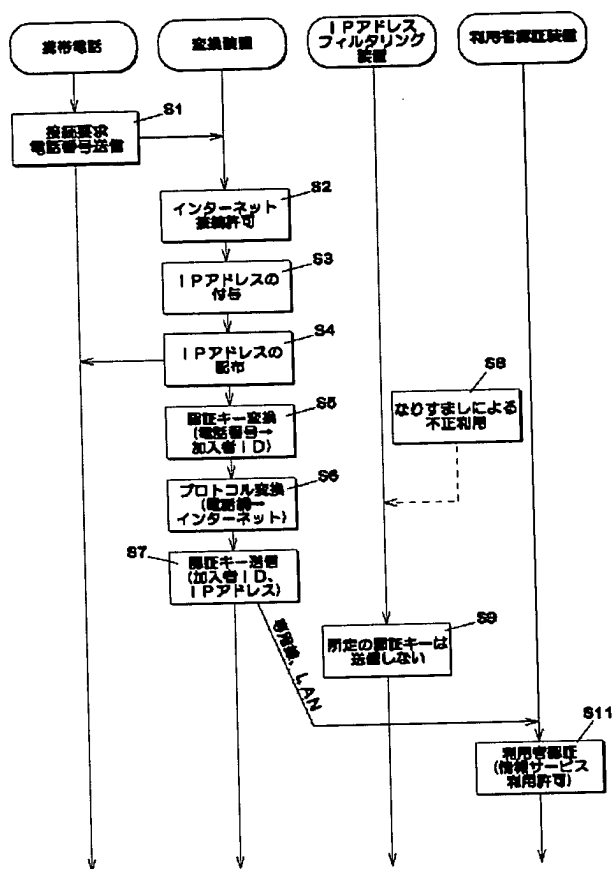
【図 4】



【図 5】



【図 6】



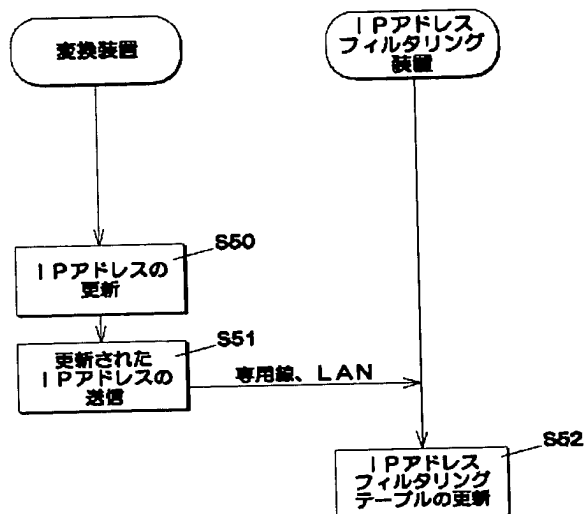
KYC00605

【図 7】

Action=R ject (禁止) Source (発信元のIPアドレス)
192.168.1.1 ? 192.168.1.200
192.168.10.1 ? 192.168.10.50
....

KYC00607

【図 8】



KYC00608

フロントページの続き

(72)発明者 大迫 哲郎

京都府京都市山科区東野北井ノ上町5番地  
の22 京セラコミュニケーションシステム  
株式会社内

Fターム(参考) 5B085 AE04 AE23 BG07

5J104 AA07 AA47 KA01 KA02 NA05

PA02 PA07

5K067 AA33 BB04 BB21 DD24 EE02

EE10 EE16 GG01 GG11 HH21

HH22 HH24